## PATENT COOPERATION TREATY

# **PCT**

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference							
	OR FURTHER ACTION	Examination Report (Form PCT/IPEA/416)					
International application No. In	ternational filing date (day/month/	vear)	Priority Date (day/month/year)				
PCT/SG 2004/000389 1	December 2004 (01.12.2	004)	24 December 2003 (24.12.2003)				
International Patent Classification (IPC) or national	al classification and IPC		(21.12.2003)				
IPC <sup>8</sup> : G06K 19/077 (2006.01); G06F		<b>3/24</b> (2	006.01)				
SINGAPORE TECHNOLOGIES LOG							
<ol> <li>This international preliminary examination report has been prepared by this International Preliminary Examination Authorit and is transmitted to the applicant according to Article 36.</li> </ol>							
2. This REPORT consists of a total of 3 sheets, including this cover sheet.							
This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have bee amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).							
	15 sheets.		•				
3. This report contains indications relating	to the following items:						
I. Basis of the opinion			•				
II. Priority							
		inventive	step and industrial applicability				
IV. Lack of unity of invent	ion .						
V. Reasoned statement und citations and explanation	der Rule 66.2(a)(ii) with regard ons supporting such statement	to novel	ty, inventive step or industrial applicability;				
VI. Certain documents cited							
VII. Certain defects in the in	ternational application						
VIII. Certain observations on	the international application						
ate of submission of the demand	Date of con	pletion o	f this report				
18.10.2005	14	4 Febr	uary 2006 (14.02.2006)				
me and mailing address of the IPEA/AT ustrian Patent Office	Authorized o	fficer					
esdner Straße 87 1200 Vienna		•	HARASEK S.				
simile No. 1/53424/200	Telephone N	n 1/53/	24/574				
n PCT/IPEA/409 (cover sheet) (July 1998)	2010phone 14		2.1101-7				

#### INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/SG 2004/000389

1		Basis of the report
1	. W	ith regard to the elements of the international application:*
		the international application as originally filed
	$\boxtimes$	the description:  pages 1,2, as originally filed  pages 3-13, filed with the demand  pages, filed with the letter of
		the claims: pages, as originally filed pages, as amended (together with any statement) under Article 19 pages, filed with the demand pages, filed with the letter of
		the drawings:  pages 1-3, as originally filed  pages, filed with the demand  pages, filed with the letter of;
		the sequence listing part of the description:  pages, as originally filed  pages, filed with the demand  pages, filed with the letter of
2.	WITH	h regard to the language, all the elements marked above were available or furnished to this Authority in the language in ch the international application was filed, unless otherwise indicated under this item.  se elements were available or furnished to this Authority in the following language which is:
		the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
		the language of publication of the international application (under Rule 48.3(b)).
		the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/ or 55.3).
3,	With preli	n regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international minary examination was carried out on the basis of the sequence listing:
		contained in the international application in printed form.
		filed together with the international application in computer readable form.
		furnished subsequently to this Authority in written form.
		furnished subsequently to this Authority in computer readable form.
		The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
		The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
		The amendments have resulted in the cancellation of:
	[	the description, pages
	Ė	the claims, Nos
		the drawings, sheets/fig
	∏ Ti t	nis report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**
in 70	this re ).17).	ment sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to eport as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and
<u>A</u>	y repl	acement sheet containing such amendments must be referred to under item 1 and annexed to this report.

Form PCT/IPEA/409 (Box I) (July 1998))

#### INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/SG 2004/000389

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement						
1. Statement	portings	and statement				
Novelty (N)	Claims	1-17	YES			
	Claims		NO			
Inventive step (IS)	Claims	1-17	YES			
	Claims		NO			
Industrial applicability (IA)	Claims	1-17	YES			
	Claims		NO			
Citations and explanations (Rule 70.	7)					

The application under consideration deals with a RFID tag arranged to function as a tamper-evident seal.

The following documents have been cited in the Search Report:

D1: US 6050622 A

D2: WO 2002/077939 A1 D3: JP 2003150924 A

All cited documents describe RFID tags that are equipped with means for the detection of tampering. Generally, tampering is detected by a change in the interrogation response of the RFID tag which in turn is due to a disruption of an electrical connection in the tag. D1 is considered to represent the closest state of the art.

In D1 tampering of the seal tag breaks the antenna of the RFID transponder. The tampered tag is therefore unable to respond to interrogation. D1 explicitly mentions several features of claim 1 of the present application such as the tag constituting a seal, the presence of an IC chip, an antenna, the ability to respond to interrogation when intact, and a line of weakness (see: fig. 11 and associated description) such that when the tag is broken along this line the RFID transponder is rendered unable to communicate. On the other hand, D1 remains silent about the described embedding of the transponder between two webs of flexible material.

Therefore, amended claim 1 and its dependent claims are considered novel and involving an inventive step. New claim 17 recites the features of original claim 18, against which no objections have been raised.

In summary, the subject-matter protection is sought for is considered to be novel and involving an inventive step. Industrial applicability is given.

the tag in place. For example, in some cases a tagged article may be removed from a container of such articles without detection by removing the tag from the article and replacing the tag in the container. In other cases, it may be that the RFID tag is applied only to the packaging of articles, and an article may thus be removed without detection simply by removing the article from the tagged package, and leaving the package within the system. At a subsequent interrogation point, the tag will respond to the interrogation device and the system will fail to detect that the article has been removed.

Subversion of the tracking and identification system is a particular problem in logistics and associated transport industries, especially those involving the transportation or movement of relatively portable items of high value, such as, for example, watches, wine, jewellery and cellular telephone handsets. Items of this type have relatively high theft rates, and thefts may involve the removal of one or more articles from a container, such as a cardboard carton, prior to sealing or resealing of the container. Accordingly, a theft may not be discovered until the container is opened at the final destination, at which time it will be difficult to determine at which stage in the supply and transportation chain the article was removed.

10

20

25

30

One method that has been employed in an attempt to detect tampering with the contents of a container is to use a tamper resistant tape to seal the container. Such tapes are resistant to resealing, and are imprinted with a pattern that is unique to the organisation responsible for sealing the container so that any attempt to cut and reseal the tape is likely to be evident upon inspection. However, rolls of the tape may be stolen or counterfeited. In any case, tampering may still not be detected until the container is inspected closely at the destination, and there remains no way to determine whether the contents of the container have been tampered with until the container has been opened.

Accordingly, there is a need for an improved apparatus and method for use in an RFID tracking and identification system that makes it more difficult to subvert the system by separating the tags from the tracked articles. It would also be desirable to provide an RFID tag for use in an RFID tracking and identification system that is convenient to apply to articles being tracked, which may be

PCT/ S0 2004/0003 {

manufactured in a straightforward manner, and which is robust in the face of normal handling and application procedures.

It is to be noted that any discussion of documents, devices, acts or knowledge in this specification is included to explain the context of the invention. It should not be taken as an admission that any of the material formed part of the prior art base or the common general knowledge in the relevant art on or before the priority date of the claims herein.

#### **SUMMARY OF THE INVENTION**

5

15

20

25

30

According to one aspect, the present invention provides an RFID tag for 10 use as a tamper-evident seal, including:

an RFID transponder having an integrated circuit chip and an antenna connected to the integrated circuit chip, the transponder being able, when intact, to communicate with an RFID interrogator device, the RFID tag having a line of weakness extending across at least a portion of the antenna or between the antenna and the integrated circuit chip, such that when the tag is broken along the line of weakness the RFID transponder is rendered unable to communicate with the RFID interrogator device;

a first web of flexible material, having an adhesive coating applied to an outer surface thereof, to enable the tag to be affixed to an article; and

a second web of flexible material,

wherein the transponder is disposed between the first and second webs of material in a laminar structure.

Accordingly, an RFID tag in accordance with the invention may be affixed to a package in such a way that it is difficult to open the package in order to remove an article contained therein, without tearing the tag along the line of weakness and thus rendering the transponder inoperable. Where the package has a line of opening, such as box having a join between a lid and body of the box or a line of meeting of flaps forming a closure in the box, a tag may be affixed to the package such that the line of weakness of the tag is aligned with the line of opening of the package. It is thus difficult to open the package along the line of opening without breaking the tag along the line of weakness.

A further advantage provided by the invention is that the first web of flexible material provides a backing giving additional strength and support to the RFID tag during handling and application, as well as providing a suitable surface for the application of the adhesive coating. The second web of flexible material provides additional protection during handling, thereby rendering the RFID tag robust to normal conditions of handling and application. Advantageously, the RFID tag of the present invention is able to be assembled by a lamination process wherein the transponder is sandwiched between at least the first and second webs of flexible material. The tag is able to be supplied in a completely self-contained form such that it may be directly applied to an article for use as a tamper-evident seal, without need for the user to provide a separate means of affixing the tag to the article.

5

10

15

20

25

30

In another aspect the invention provides a method for sealing a package in order to enable the detection of unauthorised access to the contents of the package, including the steps of:

providing an RFID tag in accordance with the invention; and

affixing the RFID tag to the package by means of the adhesive coating applied to the first web of flexible material of the tag, such that the line of weakness of the tag is aligned with a line of opening of the package,

whereby, when the package is opened along said line of opening, the tag is broken along said line of weakness.

Advantageously, if packages sealed in this manner are placed inside a larger container which is then itself sealed shut, it is then possible to interrogate the RFID tags affixed to the packages inside the container at various points in the supply and transportation chain using an RFID interrogator device. If any RFID tag fails to respond to the interrogator, it will be inferred that the corresponding article may have been tampered with or removed between successive points of interrogation.

Thus, in a further aspect the invention provides a method for detecting unauthorised tampering with, or removal of, an article stored within a container, including the steps of:

providing a plurality of RFID tags in accordance with the invention; affixing the plurality of RFID tags to the article by means of the adhesive coating applied to the first webs flexible material of the tags;

storing the article within the container;

6

subsequently interrogating the plurality of RFID tags using an RFID 8 interrogator device; and

detecting unauthorised tampering with, or removal of, the article by a failure of one or more of the RFID tags to respond to the RFID interrogator device.

5

10

15

20

25

30

The method may include the further step of providing identifying information stored within the RFID tag prior to storing the article within the container. The step of of interrogating the RFID tag may then include reading the identifying information from the RFID tag, and the step of detecting unauthorised tampering may include detecting whether the identifying information has changed since the article was stored within the container. Advantageously, this makes it difficult for a tamperer to circumvent the system by replacing a damaged tag with an intact tag, since the identifying information stored within the replacement tag would not match the original identifying information, and the change could thus be detected.

The identifying information may be transmitted electronically from a first location at which the article is stored within the container to a second location at which the RFID tag is interrogated. Thus, detecting whether the identifying information has changed may include comparing the electronically transmitted identifying information with the identifying information read from the RFID tag.

The RFID transponder may include a supporting substrate upon which the integrated circuit chip and antenna are mounted.

The first and second webs of flexible material may be made of paper. Alternatively, they may be made of a plastic such as polyvinylchloride (PVC).

In a particularly preferred embodiment, the line of weakness includes a line of perforations. Alternatively, the line of weakness may be formed in some other manner, such as by scoring the tag along the desired line. Preferably, the line of weakness is provided in the first and/or the second web of flexible material. However, in whichever manner the line of weakness is formed, it is important to ensure that the tag is not rendered inoperative, such as by severing a portion of the antenna or a connection to the integrated circuit chip.

The tag may further include one or more additional lines of weakness, each of which extends across at least a portion of the antenna or between the

## 7 PCT/ S0 2004/00038

antenna and the integrated circuit chip, such that when the seal tag is broken along any one or more of the lines of weakness the RFID transponder is rendered unable to communicate with the RFID interrogator device. The provision of multiple lines of weakness advantageously improves the flexibility of application of the tag, enabling it to be applied across lines of opening of articles having a variety of different geometries.

5

10

15

25

30

While the RFID transponder may be either active or passive, it is preferred that a passive RFID transponder be used in order to minimise the cost and complexity of the RFID tag.

In still another aspect the invention provides a method for detecting unauthorised tampering with, or removal of, an article stood within a container, including the steps of:

providing an RFID tag that includes an integrated circuit chip, an antenna connected to the integrated circuit chip, and a line of weakness extending across at least a portion of the antenna or between the antenna and the integrated circuit chip, such that when the tag is broken along said line of weakness the RFID transponder is rendered unable to communicate with a corresponding RFID interrogator device;

recording identifying information within the RFID tag;

affixing the RFID tag to the article, and storing the article within the container at a first location;

transmitting the identifying information electronically from the first location to a second location to which the container is transported;

interrogating the RFID tag at the second location using an RFID interrogation device to retrieve the identifying information stored therein; and

detecting unauthorised tampering with, or removal of, the article if either the RFID tag fails to respond to the RFID interrogator device or the retrieved identifying information does not correspond with the transmitted information.

Advantageously, this method enables a recipient of the container at the second location to verify that there is an exact match between the identifying information obtained by interrogation of the RFID tags within the container and those transmitted electronically. This enables the recipient to ensure that not only is the number of responsive RFID tags within the container correct, but that each

## PCT/ S0 2004/000389

one contains the expected identifying information, such that it would not be possible for a tamperer to circumvent the method, for example by replacing a damaged tag with an intact tag, since the identifying information of the replacement tag would not match the transmitted information.

#### 5 **BRIEF DESCRIPTION OF THE DRAWINGS**

10

15

30

Further benefits and advantages of the RFID tag of the present invention will become apparent in the following description of preferred embodiments of the invention, which should not, however, be considered to limit the scope of the invention as described in any of the preceding statements. In order that the invention might be more fully understood, embodiments of the invention will be described with reference to the accompanying drawings, in which:

Figure 1 shows an RFID tag in accordance with the invention:

Figure 2 illustrates the use of the RFID tag shown in Figure 1 to seal a package:

Figure 3 is a diagrammatic flow chart illustrating a method for detecting unauthorised tampering with a package according to the invention; and

Figure 4 shows an alternative embodiment of an RFID tag in accordance with the invention.

#### DESCRIPTION OF PREFERRED EMBODIMENT

20 An embodiment of an RFID tag 100 for use as a tamper-evident seal in accordance with an aspect of the present invention is illustrated in Figure 1. The RFID tag 100 includes an RFID transponder having an integrated circuit chip 102 and an antenna 104 connected to the integrated circuit chip. As is presently common in the art, the antenna 104 is formed as a coil antenna. The form of the RFID transponder is not critical to the invention, so long as it is sufficiently thin to 25 be readily broken in the event of tampering with an article to which it is affixed. When intact, the RFID transponder is able to communicate with an RFID interrogator device that transmits a coded RF signal, by reflecting the incident RF carrier back to the interrogator, and encoding information stored in the memory of the integrated circuit chip 102 onto the carrier in the process. The transponder shown in Figure 1 is a passive device, requiring no battery and instead deriving power from the RF signal used to interrogate the tag.

#### PCT/ SG 2004/00038 §

Suitable RFID transponders are commercially available from suppliers such as, for example, Texas Instruments. As will be appreciated by a person skilled in the art, commercial transponders are typically fabricated and supplied with the integrated circuit chip 102 and antenna 104 on an organic substrate (not shown in the figure) such as a polyester or polyimide. As shown in Figure 1, the transponder is further integrated with at least one web of flexible material 106, which provides a backing giving additional strength and support to the tag during handling and application, as well as providing a suitable surface for the application of an adhesive coating. The backing material 106 may consist, for example, of either paper or a polymer material such as PVC.

In the preferred embodiment 100, at least a second web of flexible material (not shown in the figure) is also applied over the top of the transponder to provide additional protection during handling. The complete RFID tag 100 may thus be assembled via a lamination process wherein the transponder on its substrate is sandwiched between at least two webs of flexible material such as paper or plastic.

10

15

20

25

30

The back of the RFID tag is subsequently coated with a suitable adhesive, which is preferably a strong, pressure sensitive adhesive. A release layer such as a waxed paper or plastic film will typically be applied over the adhesive to maintain its active life, and prevent the tag from adhering prematurely to other articles or surfaces. The tag may then be affixed to an article by removing the release layer and pressing the adhesive surface of the tag onto the article in the desired location.

The RFID tag 100 also has a line of weakness in the form of a line of perforations 108 that extends across a metallic conductor 110 connecting the integrated circuit chip 102 with the antenna 104. It will be appreciated that the line of weakness need not take the form of perforations, but may be formed in any suitable manner such as, for example, scoring the tag along the desired line. In whichever manner the line of weakness is created, the essential requirements are that the tag be weakened so as to be more easily torn along the line, and that the transponder not be damaged in the process of creating the line. Thus, for example, in the case of the perforated line 108 perforations may be created

10

immediately adjacent to the conductor 110, but care must be taken to ensure that no perforation is made in the conductor 110 itself.

In accordance with the invention, when the tag 100 is broken along the perforated line 110, the connection between the integrated circuit chip 102 and the antenna 104 will be severed, rendering the RFID transponder inoperable and unable to communicate with an RFID interrogator device. Accordingly, possible breakage of the tag 100 along the line 110, may be detected by attempting to interrogate the transponder. If the transponder responds to interrogation, then it may be assumed that the tag 100 has not been broken.

Figure 2 illustrates the manner in which the exemplary tag 100 may be used as a tamper evident seal on a package 200. As depicted in the drawing, the package 200 is a box having base 202 and a hinged lid 204 (the hinge being at the rear of the box, and not visible), such as a jewellery box. The box 200 therefore has a line of opening 206 running between the base 202 and the lid 204. The contents of the box 200 cannot be accessed without either damaging the box, or separating the base 202 and lid 204 along the line of opening 206 by opening the box in the usual manner.

10

15

20

25

30

The RFID tag 100 is applied as a tamper-evident seal by adhering it across the base 202 and lid 204 of the box such that the perforated line 108 is aligned with the line of opening 206. Accordingly, if the box 200 is opened, the tag 100 will break along the perforated line 108, and any subsequent attempt to interrogate the tag 100 will receive no response, providing an indication that the contents of the box 200 may have been tampered with or removed.

Advantageously, the interrogation of the tag 100 may be carried out without need for visual inspection even if the box 200 is enclosed within a larger container. Accordingly, Figure 3 illustrates diagrammatically an exemplary method in accordance with the invention that enables the detection of unauthorised tampering with, or removal of, an article stored within a container.

In a first step 302 of the method, a box 200 containing an article of value, such as jewellery, is sealed using an RFID tag in accordance with the invention, in the manner previously described with reference to Figure 2.

11

In a further step 304, the box 200 is enclosed within a larger container such as a cardboard shipping carton. The container may contain a number of individually tagged and sealed articles.

In a subsequent step 306, the container is sealed closed. It will be appreciated that a container such as a cardboard carton has a line of opening, e.g. 307, which may be sealed using ordinary packing tape, tamper resistant tape and/or a further RFID tag in accordance with the invention.

5

10

15

20

25

30

At any desired later stage 308 during shipping and handling, the contents of the container may be interrogated by an RFID interrogation device. For ease of handling, the interrogation device may, for example, be built into a surface 309 on which the container is placed, or over which the container passes, during normal processing. If all of the originally enclosed RFID tags respond to the interrogation device, it is reasonably certain that all of the corresponding articles are still enclosed within the container, and that the boxes, e.g. 200, have not been opened during handling or transit. On the other hand, failure of any of the originally enclosed RFID tags to respond to the interrogation device provides an indication that the corresponding article may have been removed and/or that the corresponding box may have been opened or otherwise tampered with. In either case, it is unnecessary to open the container or to visually inspect the contents unless an RFID tag fails to respond. Advantageously, since the container need not be opened unless tampering is already suspected, representatives of the sender, receiver or insurer of the goods may be called to be present, if desired, for the opening and inspection of the container.

To ensure security in shipment, the identifying information, otherwise known as the TagID, stored in each RFID tag may be separately transmitted, for example in electronic form, to the receiver. When the consignment is received, it is then possible for the receiver to ensure that there is an exact match between the TagID's obtained by interrogation of the RFID tags within the container and those received electronically. This ensures that not only is the number of responsive RFID tags within the container correct, but that each one contains the expected identifying information. Accordingly, it would not be possible for a tamperer to circumvent the system by replacing a damaged tag with an intact tag, since the TagID of the replacement tag would be incorrect.

12 PCT/ 90 200 4 / 00038 g

Although it is plausible in principle that a sophisticated tamperer may read the TaglD from an original tag, and program a replacement tag with the same TaglD, in practice this would be difficult, since different tags may use different protocols to communicate, and thus the tamperer would need to know the correct protocol corresponding to the tag to be read. However, even greater security could be achieved through the use of secure protocols to communicate with the RFID tags.

It will be appreciated by those skilled in the art that the RFID tag of the invention is not limited in form to the embodiment 100 described with reference to Figures 1 to 3. By way of further example only, an alternative embodiment 400 of the RFID tag is shown in Figure 4. As with the embodiment 100, the RFID tag 400 also includes an RFID transponder having an integrated circuit chip 402 and a coil antenna 404 connected to the integrated circuit chip via a conductor 410. The transponder is integrated with at least one flexible web of backing material 406 such as paper or a plastic, which has an adhesive coating on the reverse surface. The integrated circuit chip 402 is located within the perimeter defined by the coils of the antenna 404, and thus in the embodiment 400 it is not practical or convenient to form a line of weakness across the connecting conductor 410.

10

15

20

25

Thus, in the case of the alternative embodiment 400, lines of weakness are instead formed across the coils of the antenna 404. Breakage of the antenna coils will also cause the transponder to become unresponsive to interrogation. Any line that will result in breakage of the antenna will thus serve the purpose of rendering the tag inoperative, and accordingly a number of lines of weakness are provided in the alternative embodiment 400. These include a complete diagonal line 412, a horizontal line 414, a vertical line 416 and a half diagonal line 418, each of which is formed as a line of perforations. The provision of multiple lines of weakness advantageously improves the flexibility of application of the tag, enabling it to be applied across lines of opening of articles having a variety of different geometries.

To provide an even higher level of protection for articles, especially those held in large packages that may have areas of weakness or that allow access from more than one side or opening, multiple tags may be applied across the various lines or possible areas of opening. If any one of the tags applied to the

### 13 PCT/ SO 2004/00038!

package is subsequently found to be unresponsive to interrogation, this will serve to indicate that the package may have been opened or otherwise tampered with.

The above described embodiments are not intended to be limiting of the invention, and other embodiments may be implemented within the scope of the invention as defined by the appended claims.

#### 14 PCT/ SG 2004/00038!

#### **CLAIMS:**

1. An RFID tag for use as a tamper-evident seal, including:

an RFID transponder having an integrated circuit chip and an antenna connected to the integrated circuit chip, the transponder being able, when intact, to communicate with an RFID interrogator device, the RFID tag having a line of weakness extending across at least a portion of the antenna or between the antenna and the integrated circuit chip, such that when the tag is broken along the line of weakness the RFID transponder is rendered unable to communicate with the RFID interrogator device;

a first web of flexible material, having an adhesive coating applied to an outer surface thereof, to enable the tag to be affixed to an article; and

a second web of flexible material,

wherein the transponder is disposed between the first and second webs of material in a laminar structure.

- 15 2. An RFID tag according to claim 1 wherein the RFID transponder further includes a supporting substrate upon which the integrated circuit chip and antenna are mounted.
  - 3. An RFID tag according to claim 1 or claim 2 wherein the first and second webs of flexible material are made of paper.
- 20 4. An RFID tag according to claim 1 or claim 2 wherein the first and second webs of flexible material are made of plastic.
  - 5. An RFID tag according to any one of the preceding claims wherein the line of weakness includes a line of perforations.
- 6. An RFID tag according to any one of the preceding claims wherein the RFID transponder is a passive RFID transponder.
  - 7. An RFID tag according to any one of the preceding claims wherein the line of weakness is provided in the first and/or the second web of flexible material.

- 15
- 8. An RFID tag according to any one of the preceding claims further including one or more additional lines of weakness, each of which extends across at least a portion of the antenna or between the antenna and the integrated circuit chip, such that when the seal tag is broken along any one or more of the lines of weakness the RFID transponder is rendered unable to communicate with the RFID interrogator device.
- 9. An RFID tag according to any one of the preceding claims wherein the antenna is a coil antenna.
- A method for sealing a package in order to enable the detection of 10. 10 unauthorised access to the contents of the package, including the steps of:

providing an RFID tag in accordance with any one of claims 1 to 9; and affixing the RFID tag to the package by means of the adhesive coating applied to the first web of flexible material of the tag, such that the line of weakness of the tag is aligned with a line of opening of the package.

- 15 whereby, when the package is opened along said line of opening, the tag is broken along said line of weakness.
  - A method for sealing a package in order to enable the detection of 11. unauthorised access to the contents of the package, including the steps of:

providing a plurality of RFID tags in accordance with any one of claims 1 to 20 9; and

affixing the plurality of RFID tags to the package by means of the adhesive coating applied to the first webs of flexible material of the tags, such that the lines of weakness of the tags are aligned with one or more lines of opening of the package,

- 25 whereby, when the package is opened along any one or more of said lines of opening, at least one of the tags is broken along the line of weakness of the tag.
  - 12. A method for detecting unauthorised tampering with, or removal of, an article stored within a container, including the steps of:

PCT/ \$8 2004/00038

16

providing an RFID tag in accordance with any one of claims 1 to 9; affixing the RFID tag to the article by means of the adhesive coating applied to the first web of flexible material of the tag;

storing the article within the container;

subsequently interrogating the RFID tag using an RFID interrogator device; and

detecting unauthorised tampering with, or removal of, the article by a failure of the RFID tag to respond to the RFID interrogator device.

- 13. A method according to claim 12 further including the step of providing identifying information stored within the RFID tag prior to storing the article within the container, and wherein the step of interrogating the RFID tag includes reading the identifying information from the RFID tag and the step of detecting unauthorised tampering includes detecting whether the identifying information has changed since the article was stored within the container.
- 15 14. A method according to claim 13 wherein the identifying information is transmitted electronically from a first location at which the article is stored within the container to a second location at which the RFID tag is interrogated, and detecting whether the identifying information has changed includes comparing the electronically transmitted identifying information with the identifying information 20 read from the RFID tag.
  - 15. A method according to any one of claims 12 to 14 wherein the article is contained within a package, and the step of affixing the RFID tag to the article includes affixing the RFID tag to the package such that the line of weakness of the tag is aligned with a line of opening of the package, such that when the package is opened along said line of opening, the tag is broken along said line of weakness.
  - 16. A method for detecting unauthorised tampering with, or removal of, an article stored within a container, including the steps of:

25

17

providing a plurality of RFID tags in accordance with any one of claims 1 to

affixing the plurality of RFID tags to the article by means of the adhesive coating applied to the first webs flexible material of the tags;

storing the article within the container;

9;

5

10

15

subsequently interrogating the plurality of RFID tags using an RFID interrogator device; and

detecting unauthorised tampering with, or removal of, the article by a failure of one or more of the RFID tags to respond to the RFID interrogator device.

17. A method for detecting unauthorised tampering with, or removal of, an article stood within a container, including the steps of:

providing an RFID tag that includes an integrated circuit chip, an antenna connected to the integrated circuit chip, and a line of weakness extending across at least a portion of the antenna or between the antenna and the integrated circuit chip, such that when the tag is broken along said line of weakness the RFID transponder is rendered unable to communicate with a corresponding RFID interrogator device;

recording identifying information within the RFID tag;

affixing the RFID tag to the article, and storing the article within the container at a first location;

transmitting the identifying information electronically from the first location to a second location to which the container is transported;

interrogating the RFID tag at the second location using an RFID 25 interrogation device to retrieve the identifying information stored therein; and

detecting unauthorised tampering with, or removal of, the article if either the RFID tag fails to respond to the RFID interrogator device or the retrieved identifying information does not correspond with the transmitted information.